ПАМЯТКА
по противодействию телефонным мошенничествам, мошенничествам с пластиковыми картами и вредоносными программами в сети «Интернет»

За 10 месяцев 2019 года на территории Ненецкого автономного округа наблюдается рост на 7% количества преступлений, связанных с мошенничествами в отношении граждан – 92 (10-2018 – 86), из них связанных с использованием информационно-телекоммуникационных технологий – 51 (10-2018 – 45).

Самыми распространёнными способами хищений денежных средств являются:

- с помощью сети Интернет (55 или 48,2%) путем размещения сайтов «двойников» или рекламных объявлений;
- с использованием средств связи (27 или 23,7%) граждане вводятся в заблуждение под различными предлогами;
- хищение банковских карт с последующим обналичиваем денежных средств (19 или 18%).

Анализ материалов уголовных дел показывает, что все совершенные хищения допущены по невнимательности или неосведомлённости потерпевших. Жертвами преступных посягательств подвержены различные категории граждан – от пенсионеров до лиц средней возрастной группы, при этом продолжает отмечаться сдвиг в сторону лиц среднего возраста – от 20 до 40 лет.

ТЕЛЕФОННОЕ МОШЕННИЧЕСТВО

Телефонное мошенничество известно давно – оно возникло вскоре после массового распространения домашних телефонов.

В организации телефонных махинаций участвуют несколько преступников. Мошенники разбираются в психологии и умело используют всю доступную информацию, включая ту, которую жертва мошенничества невольно выдаёт при общении.

Прокуратура НАО напоминает, что чаще всего в сети телефонных мошенников попадаются пожилые люди или доверчивые подростки. При этом каждый человек может стать жертвой мошенничества, если не будет следовать простым правилам безопасности.

НАИБОЛЕЕ РАСПРОСТРАНЕННЫЕ СХЕМЫ ТЕЛЕФОННОГО МОШЕННИЧЕСТВА

Обман по телефону: требование выкупа или взятки за освобождение якобы из отделения полиции знакомого или родственника.

SMS-просьба о помощи: требование перевести определённую сумму на указанный номер, используется обращение «мама», «друг», «сынок» и т.п.

Телефонный номер - «грабитель»: платный номер, за один звонок на который со счёта списывается денежная сумма.

Выигрыш в лотерее, которую якобы проводит радиостанция или оператор связи: Вас просят приобрести карты экспресс-оплаты и сообщить коды либо перевести крупную сумму на свой счёт, а потом ввести специальный код.

Простой код от оператора связи: предложение услуги или другой выгоды – достаточно ввести код, который на самом деле спишет средства с Вашего счёта.

Штрафные санкции и угроза отключения номера: якобы за нарушение договора с оператором Вашей мобильной связи.

Ошибочный перевод средств: просят вернуть деньги, а потом дополнительно снимают сумму по чеку.

Услуга, якобы позволяющая получить доступ к SMS и звонкам другого человека.

ТАКТИКА ТЕЛЕФОННЫХ МОШЕННИКОВ

Для общения с потенциальной жертвой мошенники используют либо SMS, либо телефонный звонок.

SMS – это мошенничество «вслепую»: такие сообщения рассылаются в большом объёме – в надежде на доверчивого получателя.

Телефонный звонок позволяет манипулировать человеком при разговоре, но при таком общении можно разоблачить мошенника правильным вопросом.

Цель мошенников – заставить Вас передать свои денежные средства «добровольно». Для этого используются различные схемы мошенничества.

Изъятие денежных средств может проходить разными способами. Вас попытаются заставить:

- передать деньги из рук в руки или оставить в условленном месте;
- приобрести карты экспресс-оплаты и сообщить мошеннику коды карты;
- перевести деньги на свой счёт и ввести специальный код;
- перевести деньги на указанный счёт;
- позвонить на специальный телефонный номер, который окажется платным, и с Вашего счёта будут списаны средства.

Как правильно реагировать на попытку вовлечения в мошенничество

Мошенники очень хорошо знают психологию людей. Они используют следующие мотивы:

а. Беспокойство за близких и знакомых.

б. Беспокойство за свой телефонный номер, счёт в банке или кредитную карту.

в. Желание выиграть крупный приз.

г. Любопытство – желание получить доступ к SMS и звонкам других людей.

Чтобы противодействовать обману, достаточно знать о существовании мошеннических схем и в каждом случае, когда от Вас будут требовать перевести сумму денег, задавать уточняющие вопросы.

ЧТО НАДО ЗНАТЬ, ЧТОБЫ НЕ СТАТЬ ЖЕРТВОЙ ТЕЛЕФОННЫХ МОШЕННИКОВ

Если вы сомневаетесь, что звонивший действительно ваш друг или родственник, постарайтесь перезвонить на его мобильный телефон. Если телефон отключен, постарайтесь связаться с его коллегами, друзьями или близкими родственниками для уточнения информации.

Банки не осуществляют немедленную проверку фактов списания денежных средств с Вашей карты, либо проведение каких-либо подозрительных операций! Если Вам звонят и представляются сотрудником банка и говорят, что по Вашей карте происходят сомнительные операции – повесьте трубку и перезвоните в банк по номеру, указанному на Вашей карте.

Помните, что никто не имеет права требовать коды, присланные Вам в SMS сообщениях, и CVC код, находящийся на Вашей карте! Если у Вас просят данную информацию – это мошенники!!!

Если Вам позвонили и сообщили о выигрыше в лотерее помните – оформление выигрыша никогда не происходит только по телефону или Интернету. Если Вас не просят приехать в офис организатора акции с документами – это мошенничество.

Для возврата средств при якобы ошибочном переводе существует чек. Не возвращайте деньги – их вернет оператор.

Услуга «узнайте SMS и телефонные переговоры» может оказываться исключительно операторами сотовой связи и в установленном законом порядке.

Есть несколько правил:

- отметить в телефонной книжке мобильного телефона номера всех родственников, друзей и знакомых;
- не реагировать на SMS без подписи с незнакомых номеров;
- внимательно относиться к звонкам с незнакомых номеров.

МОШЕННИЧЕСТВО С БАНКОВСКИМИ КАРТАМИ

В последнее время наблюдается рост числа случаев мошенничества с пластиковыми картами. Прокуратура НАО рекомендует всем владельцам пластиковых карт следовать правилам безопасности:

- Никогда и никому не сообщайте ПИН-код Вашей карты. Лучше всего его запомнить. Относитесь к ПИН-коду как к ключу от сейфа с вашими средствами.

- Нельзя хранить ПИН-код рядом с картой и тем более записывать ПИН-код на неё – в этом случае Вы даже не успеете обезопасить свой счёт, заблокировав карту после кражи или утери. ВАША КАРТА – ТОЛЬКО ВАША.

- Немедленно блокируйте карту при ее утере.

- Совершая операции с пластиковой картой, следите, чтобы рядом не было посторонних людей. Набирая ПИН-код, прикрывайте клавиатуру рукой.

- Банкомат должен быть «чистым». Обращайте внимание на картоприемник и клавиатуру банкомата, они не должны быть оборудованы какими-либо дополнительными устройствами.

- Не позволяйте никому использовать Вашу пластиковую карту.

- Банкомат должен быть полностью исправным. В случае некорректной работы банкомата – если он долгое время находится в режиме ожидания или самопроизвольно перезагружается – откажитесь от его использования.

- Никогда не прибегайте к помощи либо советам третьих лиц при проведении операций с банковской картой в банкоматах. Банк обязан предоставить консультационные услуги по работе с картой.

- Не доверяйте карту официантам и продавцам. В торговых точках, ресторанах и кафе все действия с Вашей пластиковой картой должны происходить в Вашем присутствии.

ПРАВИЛА ПОВЕДЕНИЯ В ИНТЕРНЕТЕ

В Интернете действует множество мошенников, которые создают и запускают вредоносные программы.

Вредоносные программы – любое программное обеспечение, которое предназначено для скрытного (не санкционированного) доступа к персональному компьютеру с целью хищения конфиденциальных данных, а также для нанесения любого вида ущерба, связанного с его использованием.

БЕЗОПАСНОЕ ИСПОЛЬЗОВАНИЕ ЭЛЕКТРОННОЙ ПОЧТЫ

Являясь удобным видом связи, как личной, так и деловой, электронная почта остаётся одним из самых популярных способов распространения вредоносных программ в Интернете.

Обычное сообщение электронной почты – это просто текст, сам по себе он не может быть опасен. Но к сообщению можно прикрепить файл, называемый файлом вложения или файлом присоединения, который вполне может оказаться вредоносной программой или зараженным вирусом файлом.

Самый действенный способ оградить от вредоносных программ свой почтовый ящик – запретить прием сообщений, содержащих исполняемые вложения. Если абонент включает подобный фильтр, то все сообщения, содержащие исполняемые файлы, будут автоматически удаляться непосредственно на почтовом сервере.

- Во-первых, как правило, по электронной почте чаще всего рассылают документы и изображения, но не программы.

- Во-вторых, в случае необходимости получения программы по почте, можно договориться с отправителем, чтобы он предварительно упаковал ее с помощью какого-либо архиватора, например, Winzip или WinRar.

Прокуратура НАО рекомендует немедленно удалять все подозрительные сообщения.

Вредоносные программы срабатывают при запуске на Вашем компьютере.

Тактика борьбы с ними достаточно проста:

- не допускать, чтобы вредоносные программы попадали на Ваш компьютер;

- если они к Вам все-таки попали, ни в коем случае не запускать их;

- если они все же запустились, то принять меры, чтобы, по возможности, они не причинили ущерба.